A Teoria Algorítmica da Aleatoriedade

Sérgio B. Volchan

27 de agosto de 2002

Resumo

A noção de aleatoriedade é fundamental em diversas áreas da matemática pura e aplicada. Entretanto, uma definição precisa, mesmo do ponto de vista matemático rigoroso, é bastante difícil. Discutimos brevemente algumas delas, chamando a atenção para o papel central, e de certa forma surpreendente, do conceito de algoritmo e computabilidade.

1 Introdução

O que é a aleatoriedade? Existem eventos/processos aleatórios na Natureza? Faz sentido buscar leis da aleatoriedade? É possível simular a aleatoriedade?

Estas são questões muito difíceis, algumas remontando aos primórdios da investigação filosófica. Contemporaneamente, elas se situam no entroncamento entre a Filosofia, Física e a Matemática.

Uma boa medida das dificuldades envolvidas é o relativamente lento e complicado desenvolvimento da Teoria da Probabilidade, desde seus primeiros passos, cujo marco é a correspondência entre Pascal e Fermat em 1654 versando sobre jogos de azar, até a moderna axiomatização proposta por Kolmogorov em 1933. Há mesmo sugestões, baseadas em certos experimentos psicológicos, de que temos uma dificuldade de ordem cognitiva para lidar com o "acaso". Já em 1909, o matemático francês E. Borel afirmava que o ser humano é incapaz de simular aleatoriedade.

Um exemplo clássico, que mostra o quanto a intuição não é confiável nesta área, é o chamado *Paradoxo da Aleatoriedade*. Imagine o experimento que consiste em lançar uma moeda honesta (i.e., equilibrada ou perfeitamente simétrica), digamos vinte três vezes. Considere os seguintes resultados (identificando 'cara' ao dígito 0 e 'coroa' ao 1):

(1) 00000000000000000000

(2) 01101010000010011110011

(3) 11010110011100001011001

Qualquer pessoa que fosse apresentada a estes resultados diria que o primeiro é suspeito, enquanto os outros dois "parecem" aleatórios. Porquê? Note que a teoria clássica da probabilidade não nos ajuda aqui, pois os três resultados (na verdade todos os 2^{23} resultados possíveis) são equiprováveis ('moeda honesta') tendo probabilidade idêntica e igual a 2^{-23} de ocorrer.

Talvez achemos o primeiro resultado suspeito devido ao 'padrão' repetitivo e altamente regular que ele apresenta. Por outro lado, o segundo resultado, apesar de parecer irregular, consiste nos 23 primeiros dígitos da expansão binária do número $\sqrt{2}-1$, o que, por qualquer critério razoável, está longe de ser aleatório.

Quais seriam as características da aleatoriedade? Uma idéia é de associa-la a noção de *impredizibilidade*. Essa proposta baseia-se na experiência que temos com jogos de azar, como o jogo de cara e coroa. Aqui é preciso distinguir a irregularidade "local", refletida na impredizibilidade de cada jogada individual, da regularidade "global" observada, por exemplo, na tendência da freqüência relativa de caras de estabilizar-se em torno de 0,5.

Por outro lado, o lançamento de uma moeda *real* é um processo puramente mecânico, portanto sujeito às Leis de Newton. Nesse sentido, dadas as condições iniciais, o movimento está completamente determinado. A impredizibilidade nesse caso pode estar ligado a sensibilidade do sistema às condições iniciais, fenômeno conhecido como "caos determinístico".

O que descreveria então a aleatoriedade intríseca? Da noção intuitiva (e negativa) de "irregularidade" ou "ausência de padrões", surge a proposta de que aleatoriedade seria *ausência de lei*. Mas o que é uma "lei"? A fim de evitar discussões bastante complexas sobre este conceito, nos restringimos novamente aos resultados de lançamentos sucessivos de uma moeda honesta. Aqui, por 'lei' entende-se uma "lei de formação" que gera a seqüência binária dos resultados das jogadas. Neste contexto, parece razoável formalizar a idéia de lei através do conceito de *algoritmo*. Esta é a porta de entrada de noções oriundas da Lógica Matemática na discussão sobre aleatoriedade.

No que se segue discutiremos resumidamente algumas tentativas de fornecer uma definição *matemática* precisa da aleatoriedade e sua relação com a noção de algoritmos e computabilidade. Uma discussão mais detalhada e outras referências podem ser encontradas em [1].

2 Algoritmos

Queremos reponder a questão: existe uma definição matemáticamente rigorosa (e satisfatória, em algum sentido) para a noção de uma seqüência binária aleatória?

Por razões técnicas é conveniente trabalhar com o conjunto Σ das seqüências *infinitas*, na esperança de decompô-lo como união disjunta das seqüências aleatórias e não-aleatórias: $\Omega = \mathcal{R} \cup \mathcal{R}$. No caso de seqüências finitas (palavras binárias) existe a noção mais complexa de graus de aleatoriedade, que não discutiremos (ver [2]).

Para implementar a idéia de aleatoriedade como ausência de lei de formação, é preciso ter uma noção precisa desta última. A sugestão de que seqüências binárias sujeitas a uma lei de formação sejam aquelas "geradas" por um *algoritmo* parece natural hoje em dia, dada a familiaridade que temos com computadores. Entretanto, a clarificação da própria idéia de algoritmo é um desenvolvimento recente da Matemática, um subproduto

das investigações sobre fundamentos nas primeiras décadas do século XX.

É claro que a noção "intuitiva" de um algoritmo como um "procedimento efetivo" cujos passos são claramente identificados e que, se seguidos à risca, conduzem a um resultado determinado (e.g., a solução de um problema) era bem antiga. Em 1900, o matemático alemão David Hilbert incluiu na sua famosa lista de 23 problemas o de número 10, que pede (sem usar a palavra 'algoritmo') um procedimento para decidir, em um número finito de passos, se certos polinômios (ditos Diofantinos) têm solução inteira. E em 1928, junto com seu assistente W. Ackermann, ele formulou o chamado Problema da Decisão (*Entcheidugsproblem*) para a lógica formal de primeira ordem: fornecer um procedimento para decidir se uma fórmula desta é ou não um teorema.

Ora, se houvesse uma desconfiança de tais procedimentos de fato existem, para demonstrá-lo seria necessário ter uma noção precisa do que se entende por "procedimento" ou algoritmo: só assim pode-se então procurar demonstrar que não há tal receita nos problemas em questão.

Por volta de 1936, vários lógicos tais como Gödel, Church, Kleene, Post, Markov e Turing propuseram candidatos, aparentemente diferentes, para a noção de algoritmo e computabilidade. Talvez a mais simples seja a proposta de Turing. Para analisar o conceito de computabilidade ele criou uma dispositivo idealizado, a chamada Maquina de Turing (MT).

Uma MT consiste em:

- Uma fita infinita dividida em células, cada qual podendo conter um símbolo: branco, 0 ou 1;
- Uma unidade de controle (ou CPU), podendo estar em um número finito de estados internos, entre eles um estado de parada; um cursor que pode mover-se ao longo desta fita e escaneando uma célula por vez por vez.

Em cada instante, dependendo do estado corrente q da unidade de controle e do símbolo s escaneado, a máquina pode imprimir um símbolo s' (dentre 0,1 ou branco), fazer um movimento m (uma célula para esquerda ou direita) e entrar num novo estado q'. Daí o ciclo recomeça.

Assim, qualquer MT fica caracterizada pela coleção (finita) das suas instruções, i.e., quíntuplas $(q, s; s', q', m)$. Segue que a totalidade das MT é um conjunto enumeável. Assim, uma computação de uma dada MT sobre um dado 'input' p (uma palavra binária) consiste em 'rodar' o programa a partir do estado inicial com o cursor no primeiro dígito não-branco do 'input'. Se e quando e MT para, o 'output' é a palavra binária MT(p) na fita. Portanto, computação nada mais é do que manipulação de símbolos.

Logo se demonstrou que todas as diferentes propostas para a noção de computabilidade eram equivalentes, o que levou a sugestão de que se tinha encontrado a noção "correta" de computabilidade. Isso é o que afirma a famosa *Tese de Turing-Church*: um procedimento efetivo (computação ou algoritmo) é aquele capaz de ser implementado por uma Máquina de Turing. Em particular, uma função computável é aquela cujo valor, para um dado 'input' inicial, é obtido como 'output' de uma MT.

Ora, sugerimos na Introdução a identificação de aleatoriedade como "ausência de lei". Se entendermos por "lei" a lei de formação que gera os dígitos de uma seqüência binária, podemos então considerar como aleatórias aquelas não são geradas como 'output' de uma MT, i.e., como as seqüências não-computáveis.

Infelizmente essa proposta é insatisfatória, o que pode ser visto por um argumento de cardinalidade. De fato, o conjunto $\mathcal{R}$ das seqüências aleatórias seria obtido retirando de Σ todas as que são computáveis. Mas essas últimas formam um conjunto enumerável e o conjunto resultante seria grande demais. Realmente, considere as seqüências tais que $x_{2n} = x_{2n+1}$. Elas são por demais (localmente) regulares para serem consideradas aleatórias, mas como formam um conjunto não-enumerável, com certeza haveria alguma incluída em $\mathcal{R}$.

3 Aleatoriedade: três definições

Históricamente as principais noções de aleatoriedade propostas foram:

- *estocasticidade* ou *estabilidade de freqüências relativas*, devida a von Mises, Wald e Church;
- *incompressibilidade* ou *caoticidade*, devida a Solomonoff, Kolmogorov e Chaitin;
- *tipicalidade*, devida a Martin-Löf.

Vamos discuti-las brevemente.

3.1 Estocasticidade

Em 1919, von Mises, numa tentativa de fundamentar a teoria da probabilidade como parte da Física, propôs sua noção de seqüência aleatória, que chamou de "coletivos". Uma seqüência binária $x_1x_2...$ é aleatória segundo von Mises se:

(a) se f_n é o numero de 1's (ou 0's) em $x_1x_s...x_n$, então:

$$\lim_{n\to\infty} \frac{f_n}{n} = \frac{1}{2};$$

(b) a condição (a) continua valida para subseqüências.

A propriedade (a) é chamada *Lei dos Grandes Números* ou *estabilidade da freqüência relativa.* A propriedade (b) afirma que tal estabilidade é preservada sob extração (ou seleção) de subseqüências, eliminado seqüências trivialmente não-aleatórias tais como 0101010101....

É claro que (b) não pode ser válida para *qualquer* subseqüência. De fato, caso contrário dada uma $x_1x_2x_3...$ qualquer poderíamos extrair a subseqüência $x_{n_1}x_{n_2}...$ onde $x_{n_k} = 1$ para todo k violando (b), ou seja não existiria coletivo algum.

Portanto, é preciso restringir as seleções para uma classe "admissível". Uma das primeiras críticas é de que von Mises não apresentou nenhuma discussão sobre qual seria esta classe. Em 1937, Abraham Wald demonstrou que se a classe admissível for enumerável, então o conjunto dos coletivos é não-enumerável. Porém foi somente em 1940 que Alonzo Church propôs identificar as seleções admissíveis como sendo "efetivas", i.e., pela Tese de Turing-Church, com as funções computáveis.

Apesar de que os coletivos de von Mises-Wald-Church terem várias caracteríticas desejáveis para uma seqüência aleatória, ela sofreu um golpe definitivo. Em 1939 Jean Ville demonstrou que existem coletivos que não são suficientemente aleatórios, no sentido de que $\frac{f_n}{n} \geq \frac{1}{2}$ para todo n, ou seja, exibindo uma preferência de 1's sobre 0's.

3.2 Incompressibilidade

A idéia de que uma seqüência aleatória é "desestruturada" no sentido de não apresentar padões reconhecíveis, levou Ray Solomonoff, Andrei Kolmogorov e Gregory Chaitin a propor, independentemente, em meados dos anos sessenta, a noção de que tais seqüências não podem ser descritas de uma forma mais "compacta" do que exibindo a própria seqüência.

A noção-chave é a de *complexidade algorítmica* $K(x)$ de uma seqüência $x = x_1x_2x_3...$, concebida como o tamanho, em bits, do menor "programa" que "descreve" o objeto x. Por programa entende-se um código binário de uma MT que, apresentada com input nulo, começa a imprimir sucessivamente os dígitos de x.

Então, x é dita aleatória quando a complexidade $K(x_1x_2x_3...x_n)$ dos prefixos de x são da ordem de n (i.e., do tamanho mesmo do prefixo) para todo n.

Sob certos ajustes técnicos, pode-se mostrar que esta é uma noção matemáticamente rigorosa e que a vasta maioria das seqüência em Σ são aleatórias neste sentido.

3.3 Tipicalidade

Esta proposta foi desenvolvida por Martin-Löf, inicialmente como alternativa para proposta inicial de incompressibilidade que apresentava certas deficiências técnicas, por ele mesmo corrigidas posteriormente. A idéia é a de que uma seqüência aleatória não apresenta padrões reconhecíveis, i.e., deve ser "indistinta", "comum" ou "inconspícua". Em outras palavras deve ser *típica* em Σ.

Mais formalmente, $x = x_1x_2...$ é típica se satisfizer todas as "lei de aleatoriedade", i.e., todas as propriedades válidas com probabilidade um em Σ. Assim, se $\{\Sigma_\alpha : \alpha \in I\}$ for a coleção de todos os conjuntos de probabilidade um, então x é típica se pertence a $\cap_{\alpha \in I}\Sigma_\alpha$.

Esta noção só é consistente sob certas condições técnicas, particular, tem-se que incluir somente os conjunto *efetivamente* ou *computavelmente* de probabilidade um. Uma interpretação alternativa: x é típica se passa em todos os "testes estatísticos efetivos" (ver [3]).

Um resultado surpreendente é o *Teorema de Levin-Schnorr* (1974), que prova a equivalência desta noção com a de incompressibilidade, i.e.: $x \in \Sigma$ é típica se, e somente se, é incompressível.

4 Conclusão

A definição matemáticamente rigorosa e consistente de seqüência aleatória: a noção de tipicalidade de Martin-Löf. Ela coincide com outra definição, aparentemente diferente, de incompressibilidade. Esta descoberta, combinada com o fato de nenhuma contradição ter sido decoberta, é forte indício em favor de adota-la como a definição "correta" de aleatoriedade.

Talvez a maior crítica a ser feita é o fato das definições, todas negativas, dependerem crucialmente da noção de computabilidade, herdada da Tese de Turing-Church. Por outro lado, até o presente não surgiu alternativa mais adequada.

Por outro lado, não está claro a relevância desta definição no que diz respeito a aleatoriedade no mundo natural, e.g., em Física.

Referências

[1] Volchan, S. B., *What is a random sequence?*, American Mathematical Monthly, Vol. 109, no. 1, january 2002, pg. 46-63.

[2] Li, M. e Vitányi, P., *An Introduction Kolmogorov Complexity and Its Applications*, Springer-Verlag, 2^{nd} edition, 1997.

[3] Denker, M. e Woyczyński, W. A., *Introductory Statistics and Random Phenomena*, Birkhäuser, 1998.

Sérgio B. Volchan
Deptartamento de Matemática, Pontifícia Universidade Católica do Rio de Janeiro, Rua Marquês de São Vicente 225, Gávea, 22453-900 Rio de Janeiro, Brasil
volchan@mat.puc-rio.br